ИТ–ТЕХНОЛОГИИ, МАТЕМАТИЧЕСКИЕ МОДЕЛИ И ЭКОНОМЕТРИКА В ОРГАНИЗАЦИИ И УПРАВЛЕНИИ БИЗНЕСОМ

УДК 004.5

ЧЕЛОВЕЧЕСКИЙ ФАКТОР В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВ

Бойченко Олег Валериевич, д.т.н., профессор,
Акинина Людмила Николаевна, старший преподаватель,
Иванюта Дмитрий Викторович, магистрант,
Крымский федеральный университет им. В.И.Вернадского
Boychenko Oleg, prof., bolek61@mail.ru
Akinia Luidmila Nikolaevna, teacher, akininal18@mail.ru
Ivanyuta Dmitriy, m., d.iwanyuta2011@yandex.ua
V. I. Vernadsky Crimean Federal University

Аннотация. В статье исследуется влияние человеческого фактора на информационную безопасность банков, проведен анализ его влияния на безопасность функционирования автоматизированных систем управления банковской деятельностью с целью разработки инструмента предотвращения угроз для банковских информационных технологий.

Ключевые слова: человеческий фактор, банки, информационные технологии, защита информации, информационная безопасность, инциденты, угрозы.

В последнее время проблема защиты информации приобрела большое значение не только в информационной безопасности банков, но и в системе национальной безопасности государства. В мировой практике уже известны случаи нападения на информационные системы государственных органов и предприятий, кибератаки на системы электронной переписки государственных лиц и организаций, политических партий и учреждений. Причем количество кибератак постоянно растет.

«Периодические всплески хакерской активности наблюдаются в различное время и в различных масштабах, примером чего может быть недавнее важнейшее событие в жизни нашего государства– выборы президента Российской Федерации 18 марта 2018 года. Так, хакерские атаки были совершены на государственную автоматизированную систему «Выборы», в частности сайт ЦИК РФ и информационно–справочный центр в день выборов президента подвергся DDoS–атаке с IP–адресов из 15 стран» [1, с.15].

К техническим решениям проблем безопасности банков, прежде всего, можно отнести брандмауэры, антивирусное программное обеспечение, VPN и SIEMS. Однако, только технические элементы управления не могут гарантировать на практике информационную безопасность и создать эф-

фективную форму контроля безопасности, так как в технологическом подходе имеются следующие недостатки:

– ошибки и пробелы в технологиях (несмотря на постоянное совершенствование программного обеспечения, злоумышленники продолжают находить уязвимости, поскольку даже многослойная безопасность не является идеальной: каждый слой имеет свои уязвимости);

– пользователи не имеют полного представления о проблемах информационной безопасности. Например, используя стандартное антивирусное программное обеспечение, сканируя письма на наличие вирусов, пользователи часто игнорируют возможность атак на карты памяти USB, JavaScript, DNS и другие;

– значительные расходы на технологии безопасности, сделанные на заказ, при этом стандартные пакеты не дают должного преимущества;

– отсутствие специалистов, способных внедрять, эксплуатировать, управлять и обслуживать системы с целью обеспечения безопасности технологий.

Таким образом, при технологическом подходе к решению проблемы не исключена возможность нарушения системы безопасности банков, в связи с тем, что не рассмотрены и не проанализированы угрозы безопасности, связанные с человеческим фактором.

Ранее применение технологий рассматривалось как единственно необходимый подход для принятия решений, направленных на предотвращение угрозы банковских информационных технологий. При этом исследованиям по изучению в этом направлении человеческого фактора не придавалось должного значения, поэтому они были ограничены. Однако в обеспечении безопасности существуют вопросы, которые в основном касаются людей, а не технологий и важность этого направления трудно переоценить. При технологическом контроле безопасности системы возможны некоторые ошибки, которые могут сделать систему уязвимой. Однако человеческая ошибка способна вызвать более серьезные нарушения безопасности. Даже техническую ошибку можно рассматривать как результат действий человека.

«Исследование безопасности от Cisco Systems показало, что пользователи, которые работают дистанционно, все равно будут участвовать в действиях, которые угрожают системе безопасности. Изучение поведения сотрудников показало, что, получив подозрительное электронное письмо, 37% не только откроют электронную почту, но и пройдут по ссылке, в то время как 13% откроют прикрепленный файл. Кроме того, после получения обычного письма, 42% переходили по ссылке и предоставляли конфиденциальную информацию, а 30% открывали файл, который предположительно улучшил бы производительность компьютера» [2].

Для обеспечения достойной защиты информационных ресурсов государственных органов, банков, предприятий необходимо учитывать влияние человеческого фактора, поэтому при разработке IT–систем специалисты обязательно принимают меры по обеспечению безопасности с целью предотвращения ее уязвимости и возможной эксплуатации злоумышленниками.

Другим способом получения доступа к конфиденциальной информации является использование уязвимости людей, с учетом их слабых сторон, которые выявляют, изучая особенности поведения.

Наличие достаточно функциональных брандмауэров предполагает, что они правильно настроены и поддерживаются людьми. Аналогично, и антивирусная защита, и другие технологии безопасности предполагают правильную настройку с учетом меняющихся угроз. Именно человек приобретает и настраивает системы, включает функции управления, проводит мониторинг возможных угроз и уязвимостей системы.

При работе человека с компьютером выделяют две категории факторов, влияющих на безопасность компьютера: человеческий и организационный.

Человеческий фактор делят на следующие группы [2]:

1. Факторы, которые относятся к управлению, а именно рабочая нагрузка и некачественная работа персонала;
2. Факторы, связанные с конечным пользователем.

В современном обществе сотрудники банков и других организаций могут оказаться слабым звеном в обеспечении защиты информационных ресурсов.

Перечислим наиболее популярные угрозы безопасности информационной системы, которые связаны с действиями человека [3]:

– нарушение правил эксплуатации автоматизированных рабочих мест;

– утрата носителей информации, содержащих ценные для организации сведения;

– утечка информации через сеть Интернет;

– разглашение защищаемой информации третьим лицам.

Нельзя забывать и о вреде, который могут нанести инсайдеры, внедрившись в организацию с целью хищения или нарушения целостности информации.

Статистика показывает, что большинство угроз безопасности информационных систем исходят от самих сотрудников и связаны с их некачественной подготовкой и халатностью. К примеру, использование компьютерных гаджетов и отсутствие у сотрудников базовых знаний относительно безопасного использования устройств во время работы в сети Интернет может сделать информационную систему уязвимой для киберугроз. Эту проблему необходимо решать путем обучения сотрудников умению безопасного пользования гаджетами, регламентированным доступом в Интернет, запретом на посещение нежелательных сайтов и использование ненадежных серверов. Работа, проведенная в этом направлении, позволит значительно уменьшить число случайных утечек и защитить информационную систему от фатальных последствий, связанных с кибервзломами.

Человеческий фактор можно рассматривать как важнейший этап обеспечения безопасности государства и личности. Не вызывает сомнений, что современные программные и аппаратные средства информационной безопасности не всегда способны защитить информационные ресурсы от элементарной человеческой невнимательности и халатности.

Приведем некоторые рекомендации для специалистов, имеющих доступ к государственным и корпоративным данным:

1) пароль от операционной системы или электронной почты должен представлять собой несвязную комбинацию из цифр и символов длиной более 12 символов;

2) пароль не должен находиться на рабочем месте пользователя (в частности нельзя приклеивать его на монитор), так как значение такого пароля теряет всякий смысл;

3) нельзя открывать все гиперссылки от знакомых и незнакомых людей, не просмотрев сроки и типы доменов, например «Odnoclassniki.ru» могут выдавать за «Odnoklassniki.ru»;

4) не следует отвечать без предыдущей проверки на запросы администраторов и провайдеров в случае утери пароля или других данных пользователя системы или сети, потому что такой метод чаще всего используют злоумышленники;

5) нельзя использовать пиратское программное обеспечение, которое может содержать маскированные вирусы.

Изучив наиболее распространенные типы угроз информационной безопасности в компьютерных сетях, приходим к заключению относительно определяющей роли человеческого фактора в защите информации. Качественная профессиональная подготовка сотрудников предприятий, учреждений, организаций определяет информационную безопасность корпоративного и государственного сектора.

Отдельно хочется рассмотреть действие человеческого фактора в работе банков и компаний.

Сегодняшняя практика показывает, что, недооценив влияние человеческого фактора и при отсутствии проведения специальной работы с сотрудниками в период внедрения передовых автоматизированных систем, можно поставить под удар процесс реализации проекта и общее благополучие всей компании. Основные риски, которые могут возникнуть в этом случае: незавершенность проектов, потеря компетентных специалистов, отказ ИТ–специалистов поддерживать внедрение новых автоматизированных систем, сопротивление нововведениям сотрудниками.

Недооценив эти риски, можно внедрять информационные системы, которые не будут использоваться сотрудниками, что приведет к серьезным финансовым потерям.

Учитывая, что внедрение новейших автоматизированных систем – это достаточно сложный и многогранный процесс, желательно вести грамотную разъяснительную работу о необходимости функционирования этих систем с созданием благоприятных условий для приобретения полезного опыта и повышения своей квалификации при освоении новых технологий

Так как в современном мире идет постоянная борьба между хакерами и специалистами по информационной безопасности, следует помнить, что основным источником инцидентов, возникающих из–за человеческого фактора, является недостаток необходимой информации и ограниченность ресурсов для организации противодействия угрозам. Также необходимо учи-

тывать психологические и физиологические реакции человека, подтверждением которых служат ситуации, которые моделирует социальная инженерия.

В процессе реагирования на инциденты люди часто являются слабым звеном, а непредсказуемость поведения человека может уничтожить самые безопасные информационные системы. Человеческий фактор способен нарушить защиту системы вследствие неадекватных действий сотрудников, которые могут быть результатом: невозможности выполнения человеком порученных ему работ вследствие перегруженности, преднамеренные действия сотрудника, которые нарушают правила функционирования системы и могут являться следствием адаптации человека к среде или его убеждений, некомпетентность сотрудника

Для полноценного обеспечения информационной безопасности в деятельности банков, необходимо учитывать, что человеческие факторы и технические одинаково важны. Качественное управление рисками возможно при постоянном анализе угроз, уязвимостей, воздействий и совершенствовании системы контроля.

Таким образом, информационная безопасность – это постоянный процесс управления. По нашему мнению, любой организации необходимо обеспечить надлежащий контроль пользователей информационных систем. Эту проблему предлагаем решить путем формирования у сотрудников четкого понимания важности информации, с которой они работают, разъяснения о существующих и потенциальных угрозах, анализа произошедших инцидентов. Все эти мероприятия будут способствовать повышению у сотрудников информационной грамотности, что должно привести к снижению количества инцидентов безопасности.

Список использованных источников:

1. Бойченко, О.В. Защита персональных данных пользователей / О.В. Бойченко // Теория и практика экономики и предпринимательства: XV Междунар. науч.–практ. конф. (Симферополь–Гурзуф, 2018), 19– 21 апреля 2018 г.: тезисы докладов. – С. 15–16.

2. Человеческий фактор в информационной безопасности – Хабр. – 2017 г. – (https://habr.com/post/344542/)

3. Кошелев С. О., Яцкевич А. И. Информационная безопасность и человеческий фактор // Молодой ученый. — 2016. — №7. — С. 17–19. — URL https://moluch.ru/archive/111/27330/.